

Hamming's Original Paper Rewritten in Symbolic Form: A Preamble to Coding Theory

H. Gopalakrishna Gadiyar and R. Padma

School of Advanced Sciences, V. I. T. University, Vellore 632 014, India

E-mail: {gadiyar, rpadma}@vit.ac.in

Abstract

In this note we try to bring out the ideas of Hamming's classic paper on coding theory in a form understandable by undergraduate students of mathematics.

1 Introduction

Long ago Brinn [5] made an appeal for introducing algebraic coding theory in the undergraduate curriculum. This goal is more urgent now than ever with the ubiquity of computers and communication devices. This article is still worth reading though it was written thirty years ago.

The aim of this note is to write Hamming's paper in symbolic form. Hamming used the deceptively simple idea of interleaving parity check which helps to locate and hence correct errors.

This note will enable readers to move on to the now classic books by V. Pless [9] and Berlekamp [1]. Hamming's classic paper [6] is difficult to read because the mathematics is written in words and tables. This was because the audience of mathematicians and engineers in those days who worked in applied fields preferred to avoid symbolic notation and algebra as far as possible. This situation has completely changed due to various reforms in the curriculum.

In the books by Birkhoff [3] and Pless [9], a more sophisticated approach is used where the group property of the codes is emphasized as this leads to the more recent developments. The parity check bits are not interleaving but an identity matrix appended to the end.

Our simple minded approach of translating Hamming's paper into symbolic form is to enable undergraduate students to understand the elegance and simplicity of Hamming's construction which is a mix of engineering

thinking and mathematical thinking. The concepts of interleaving and parity check have their origin in engineering. The idea of coding belongs more to pure mathematics. Understanding Hamming's paper is essential for reading the book "From error correcting codes through sphere packings to simple groups" by Thomas M. Thompson [10] which is a delightful mix of history and pedagogy. This would enable undergraduate students to appreciate the unity of pure and applied mathematics, interdisciplinary and multidisciplinary research through this concrete example given in historical form. It would also enable them to take the more standard route for pursuing further developments in algebraic coding theory.

2 Hamming's construction

Parity bits are an engineering trick to detect errors in a string of 0's and 1's. In its simplest form the number of 1's is counted and then computed modulo 2. The answer would be 0 if the number of 1's is even and 1 if the number of 1's is odd. This is appended to one end of the binary string. In Hamming's case he interleaves the parity check bits in a clever way for error correction. This is a conceptual leap beyond error detection which was well known then.

Let m be the number of information bits, k the number of error correction bits and $n = m + k$. Since any k bits represent numbers from 0 to $2^k - 1$, we need the condition that $2^k - 1 \geq n = m + k$. Hence if a single error has occurred, one can determine its position from the k -bit binary representation of its position number (Hamming calls it Checking number.) Hamming interleaves the k check bits in positions $x_{2^0}, x_{2^1}, \dots, x_{2^{k-1}}$. He places the $m = n - k$ information bits at the remaining positions. Hamming analyzed the case of $(7, 4)$ code with the rate $\frac{4}{7} \sim 0.571$ in the modern notation. In the notation given above, $k = 3$, $m = 4$ and $n = 7$.

The k check bits are calculated as follows. At the encoding end, $x_1 = x_{2^0}$ is determined by the partial parity check equation

$$x_1 + x_3 + x_5 + x_7 + \dots = 0 \tag{1}$$

Notice that all these bits have their position numbers 1, 3, 5, 7 \dots which when they are written in their binary representation have the least significant bit equal to 1. Hence if the single error has occurred in any one of the odd

positions, then at the decoding end, the partial parity check equation will give

$$x_1 + x_3 + x_5 + x_7 + \cdots = 1 \quad (2)$$

Next, x_2 is determined (at the encoding end) by the equation

$$x_2 + x_3 + x_6 + x_7 + \cdots = 0 \quad (3)$$

Notice that the binary representations $(10, 11, 110, 111, \dots)$ of the position numbers of $2, 3, 6, 7, \dots$ have 1 as their second bit from the right and 2 is the smallest of these numbers. Hence if the single error has occurred in a position whose second bit is 1, then at the decoding end, we would get

$$x_2 + x_3 + x_6 + x_7 + \cdots = 1 \quad (4)$$

Similarly $x_{2^2}, \dots, x_{2^{k-1}}$ are determined by the corresponding partial parity check equations. Notice that $1, 2, 4, 8, \dots, 2^{k-1}$ ($1, 10, 100, 1000, \dots, 100 \dots 0$) are the smallest numbers having 1 in the first, second, third, fourth, $\dots k^{th}$ positions in their binary representations. Thus the position number of the error bit is determined bit by bit from right to left. The least significant bit is zero if (1) is true and 1 if (2) is true. Similarly the previous bit is zero if (3) is true and 1 if (4) is true and so on. Once the position of the error bit is found, the bit can be corrected as a bit can take only two values: 0 or 1.

At this point we would encourage the reader to look at the classic paper of Hamming paper [6] which is freely down loadable from the Internet and then read the standard books listed below.

3 Pedagogical and historical comments

[11] uses symbolic notation for bits with parity check matrix but the idea of interleaving is missed. [8] also does not talk about interleaving parity check bits. [3] and [11] discuss Hamming codes as a special case of group codes.

References

- [1] E. R. Berlekamp, *Algebraic coding theory*, McGraw - Hill, 1968.
- [2] E. R. Berlekamp, *Key papers in the the development of Coding theory*, Ed: E. R. Berlekamp, IEEE Press, 1974.

- [3] G. Birkhoff and T. C. Bartee, *Modern applied algebra*, McGraw - Hill, 1970.
- [4] Ian F. Blake, *Algebraic Coding theory: History and Development*, Dowden, Hutchinson & Ross, 1973
- [5] L. W. Brinn, *Algebraic coding theory in the undergraduate curriculum*, American Math. Monthly, **91**, 8 October, 1984, 509-513.
- [6] R. W. Hamming, *Error detecting and error correcting codes*, The Bell System Technical Journal, **29** April 1950, 147-160.
<http://www3.alcatel-lucent.com/bstj/vol29-1950/articles/bstj29-2-147.pdf>
- [7] R. Hill, *A first course in coding theory*, Oxford University Press, 1986.
- [8] W. C. Huffman and V. Pless, *Fundamentals of error correcting codes*, Cambridge University Press, 2003.
- [9] V. Pless, *Introduction to the theory of error correcting codes*, Wiley - Interscience Series in Discrete Mathematics and Optimization, 1998.
- [10] T. M. Thompson, *From error correcting codes through sphere packings to simple groups*, Cambridge University Press, 1983.
- [11] J. P. Tremblay and R. Manohar, *Discrete Mathematical Structures with applications to computer science*, McGraw-Hill Interamericana, 1975.